



TITLE:

根号による1の n 乗根の解法(数式処理と数学研究への応用)

AUTHOR(S):

元吉, 文男

CITATION:

元吉, 文男. 根号による1の n 乗根の解法(数式処理と数学研究への応用). 数理解析研究所講究録 1986, 581: 1-6

ISSUE DATE:

1986-02

URL:

<http://hdl.handle.net/2433/99314>

RIGHT:

根号による 1 の n 乗根の解法

電子技術総合研究所 元吉文男 (Fumio Motoyoshi)

1. はじめに

1 の n 乗根は任意の正数 n に対して根号によって表わされることが知られているが、これを実際に計算機で求めるプログラムを作成したので報告する。この際、従来から知られていた方法に手を加え、計算量を考慮したアルゴリズムになるようにした。また根号の扱いについても計算機で機械的に処理するのに適した解釈をするようにした。ここでは、まずこの根号の解釈法を述べ、次に 1 の n 乗根を求める実際のアルゴリズムを解説する。最後にこのアルゴリズムによって求められた 1 の 7 乗根と 13 乗根をしめしておく。

2. 根号の解釈

x の n 乗根 $a = \sqrt[n]{x}$ というのは n 乗して x になる数のことであるが、このような数は n 個あり、a によってそのうちのどれを表わすかが問題となる。x が正の実数のときは普通は a は正の実数になるようにしている。しかし x が複素数のときにはどれにするかが明らかではない。主値をとるという偏角を最小にする方法もあるが、これでも問題が生じることがある。たとえば 3 次方程式 (1) が与えられたときに、 t_1 と t_2 を (2) で示さ

$$x^3 + p x + q = 0 \quad \dots \dots \dots (1)$$

$$t_1 = -\frac{q}{2} + \sqrt{\left(\frac{p}{2}\right)^2 + \left(\frac{q}{3}\right)^3}, \quad t_2 = -\frac{q}{2} - \sqrt{\left(\frac{p}{2}\right)^2 + \left(\frac{q}{3}\right)^3} \quad (2)$$

$$x = \sqrt[3]{t_1} + \sqrt[3]{t_2} \quad \dots \dots \dots (3)$$

れる値としたときに、(3)で示される x が根であるとするが、このときには t_1 の3乗根と t_2 の3乗根のとりかたは独立ではなく、その積が $-p/3$ であるという関係がある。そこでいつも主値をとるようにしていたのでは不都合が生じる。

ここでは根号を次のように解釈することにする。すなわち、根号で示される式は、そのどの分岐をとってもよいようにする。ただしいったん分岐を定めたならば、次からは同じ式が根号の中に入る場合には前と同じ分岐をとることにする。この条件はもうすこし緩めることが可能で、実際、同じところで根号をとったものだけを同じ分岐にするようにしても以後の計算に不都合は生じない。しかし、これでは出力のときにどの根号どうしが同じ分岐であるかをいちいち指定しなくてはならず不便であるので最初に述べた方策に従うことにした。ただし、こうすることによって上の例における(3)式のような書き方が許されなくなる。すなわち、(3)における2つの根号は分岐のとりかたが相互に依存しているからである。ここでの根号の解釈の仕方によると、(3)の根は次のように表わすことになる。

$$x = \sqrt[3]{t_1} - \frac{p}{3\sqrt[3]{t_1}} \dots\dots\dots (4)$$

すなわち、分岐のとりかたが依存しているような根号は一つの根号で表わさなければならない。(4)式では分岐のとりかたによって自動的に3つの根が表現されている。

3. “1”の原始 n 乗根の解法

1の原始 n 乗根を ω_n とする。原始 n 乗根というのは次の式を満たす数のことである。

$$\omega_n^n = 1 \quad \text{かつ} \quad \omega_n^m \neq 1 \quad 0 < m < n.$$

まず n が素数の場合に帰着されることを示す。

I. $n = p^k$ のとき (p は素数)

$\omega_n = \sqrt[k]{\omega_p}$ が1の原始 n 乗根となる(どの分岐をとっても)。

II. $n = pq$ のとき (p と q は互いに素)

$x = \omega_p \omega_q$ を考える。このとき、 $\omega_p = \omega_{pq}^q = \omega_n^q$ 、 $\omega_q = \omega_{pq}^p = \omega_n^p$ と書ける。

すると $x = \omega_n^{p+q}$ となるが、 $\gcd(n, p+q) = 1$ なので

x が 1 の原始 n 乗根である。

n が素数でない場合は上の 2 つで尽くされており、これらを繰り返し適用することによって、 n が素数の場合に帰着される。 n が素数の場合の解法を以下に示すが、そこでは、前節で述べた根号の解釈にあてはまるようになっており、分岐のとりかたが相互に依存する根号が存在しないようになっている。

ω_n を 1 の原始 n 乗根とすると、 n が素数の場合は R を有理数としたときに $G(R(\omega_n), R)$ が $n-1$ 次の巡回群になる。ここで $G(A, B)$ は体 B の上の体 A のガロア群である。このとき、 $G_0 = G(R(\omega_n), R)$ とすると次のような可解列 G_i が存在する：

$$G_0 \supset G_1 \supset \cdots \supset G_m = e,$$

ただし G_{j-1}/G_j は素数次の巡回群 ($0 < i \leq m$)。

各 G_j に対応する体をそれぞれ R_j として G_{j-1}/G_j の次数を p_j とおくと、 $R_{j-1} = R_j(\eta_j)$ となっている。ここで η_j は G_j 上のある既約 p_j 次方程式の根である。この方程式を求め、それをラグランジェの分解式を使用して解けばよい。以下に述べる方法では、方程式を求める部分とそれを解く部分をまとめてある。そのため、方程式は直接には表われて来ない。

III. n が素数のとき

次のような整数列 f_j を求める：

$$n-1 = f_0 > f_1 > \cdots > f_m = 1,$$

ただし、各 f_j は f_{j-1} を割り切り、 $p_j = f_{j-1}/f_j$ は素数であり、

かつ $p_{j-1} \geq p_j$ とする ($1 \leq j \leq m$ について)。

$$e_j = (n-1)/f_j \text{ としておく。}$$

2) n の原始根を r とし、 $\zeta_0 = \omega_n$ 、 $\zeta_{i+1} = \zeta_i^r$ とする

$$(0 \leq i < n-1)$$

ここでの計算は ω_n を変数とみなして、 ω_n に関する多項式として計算を進める。

なおこの計算の際に ω_n の n 次以上の項は次の関係により消去することができる。

$$\omega_n^n - 1 = 0$$

以後の計算においても同様に行う。

$$\begin{aligned} 3) \quad \eta_{0,0} &= \zeta_0 + \zeta_1 + \cdots + \zeta_{n-2} \\ &= \omega_n + \omega_n^2 + \cdots + \omega_n^{n-1} \\ &= -1 \end{aligned}$$

とし、次のことを各 j について行う ($1 \leq j \leq m$)。

3. 1) 1) における e_j, e_{j-1}, f_j を使用して

$$\begin{aligned} \eta_{j,i} &= \zeta_{ie_{j-1}} + \zeta_{e_j + ie_{j-1}} + \cdots + \zeta_{(f_j-1)e_j + ie_{j-1}} \\ (0 \leq i < p_j) \end{aligned}$$

を計算する (ガウスの f_j 項周期)

3. 2) $\eta_{j,0}$ を次の手順に従って求める。

i) I I I の手続きを再帰的に使用して 1 の原始 p_j 乗根 ω_{p_j} を求める。

ii) ラグランジュの分解式を次のように求める。

$$\langle \omega_{p_j}^k, \eta_j \rangle = \sum_{i=0}^{p_j-1} \omega_{p_j}^{ik} \eta_{j,i} \quad \text{と定義する。} \cdots \cdots (*)$$

$$\text{このとき } \langle \omega_{p_j}^0, \eta_j \rangle = \sum_{i=0}^{p_j-1} \eta_{j,i} = \eta_{j-1,0} \text{ である。}$$

また $u_{j,k} = \langle \omega_{p_j}^k, \eta_j \rangle \langle \omega_{p_j}, \eta_j \rangle^{p_j-k}$ は ω_n の多項式であるが、

これは $\eta_{j-1,0}$ を表わす ω_n の式を使用して ω_n を消去できることが知られている ($1 \leq k < p_j$)

$\eta_{j-1,0}$ はすでに根号で表わされているので $\eta_{j,k}$ も根号で表わせる。

この $u_{j,k}$ を使用して

$$\langle \omega_{p_j}, \eta_j \rangle = \sqrt[p_j]{u_{j,1}}$$

がまず求まり、

$2 \leq k < p_j$ については

$$\langle \omega_{p_j}^k, \eta_j \rangle = u_{j,k} \langle \omega_{p_j}, \eta_j \rangle^{p_j-1} = u_{j,k} \langle \omega_{p_j}, \eta_j \rangle^k / u_{j,1}$$

によって求まる。

ここで (*) の式について 0 から $p_j - 1$ まで加えると、

$$p_j \eta_{j,0} = \sum_{k=0}^{p_j-1} \langle \omega_{p_j}^k, \eta_j \rangle$$

となり、 $\eta_{j,0}$ が根号によって表わされる。

4) 3) によって求めた $\eta_{j,0}$ が 1 の原始 n 乗根 である。

注)

3) における繰り返しにおいて最後の $j = m$ の場合は実は次のように簡単に計算できる。

n は 2 と異なる素数と考えてよいので、 $n - 1$ は偶数となり

$f_{m-1} = 2$ となる。このとき $r^{n-1} = 1 \pmod{n}$ から

$r^{(n-1)/2} = -1 \pmod{n}$ がいえるので

$$\eta_{m-1,0} = \xi_0 + \xi_{(n-1)/2} = \omega_n + \omega_n^{r^{(n-1)/2}} = \omega_n + \omega_n^{-1}$$

となり これを変形して

$$\omega_n^2 - \eta_{m-1,0} \omega_n + 1 = 0$$

となるので、直ちに解くことができ、次の式が得られる：

$$\omega_n = (\eta_{m-1,0} + \sqrt{\eta_{m-1,0}^2 - 4}) / 2.$$

4. 例

3 で述べたアルゴリズムを使用して実際に 1 の 7 乗根と 13 乗根を計算した例を次ページに示す。そこで使用されている記号について説明する。

$W(n)$ は ω_n を示す。1 つの式にすると長すぎるので根号の中が数字でない場合には、@2 などと書いて後でその値を示している。根号は | で表わし

$|x$ は \sqrt{x} を、 $n | x$ は $\sqrt[n]{x}$ を表わすものとする。また x^n は x^n を表わす。

$$W(7) = (4 \cdot 102 + 3 \cdot 13 \cdot i \cdot 3 \cdot 101^2 + 3 \cdot 101^2 + 28 \cdot 3 \cdot 101 - 56) / 336$$

$$101 = 28 (-3 \cdot 13 \cdot i + 1)$$

$$102 = 21 (-13 \cdot i \cdot 3 \cdot 101^2 + 2 \cdot 3 \cdot 101^2 + 7 \cdot 13 \cdot i \cdot 3 \cdot 101 - 7 \cdot 3 \cdot 101 - 196)$$

$$W(13) = (2 \cdot 105 + 4 \cdot 104 + 3 \cdot 13 \cdot i \cdot 3 \cdot 103^2 - 5 \cdot 3 \cdot 103^2 + 52 \cdot 3 \cdot 103 - 104) / 1248$$

$$103 = 52 (-3 \cdot 13 \cdot i - 5)$$

$$104 = 39 (-3 \cdot 13 \cdot i \cdot 3 \cdot 103^2 - 8 \cdot 3 \cdot 103^2 - 39 \cdot 13 \cdot i \cdot 3 \cdot 103 + 13 \cdot 3 \cdot 103 + 676)$$

$$105 = 2 (3 \cdot 13 \cdot i \cdot 3 \cdot 103^2 \cdot 104 - 5 \cdot 3 \cdot 103^2 \cdot 104 + 52 \cdot 3 \cdot 103 \cdot 104 - 104 \cdot 104 - 312 \cdot 13 \cdot i \cdot 3 \cdot 103^2 - 156 \cdot 3 \cdot 103^2 - 20 \cdot 28 \cdot 13 \cdot i \cdot 3 \cdot 103 - 2028 \cdot 3 \cdot 103 - 105456)$$

記号の意味:

x^n は x^n ,

$|x$ は \sqrt{x} , $n|x$ は $\sqrt[n]{x}$ を表わす